

# **EMGT 835 FIELD PROJECT**

## ***Protecting a University's Wireless Data Network with the WPA and VPN Security Solutions***

**By**

***Tee – Rattanachai Saksupakul***

**Master of Science**

**The University of Kansas**

***Spring Semester 2007***

**An EMGT Field Project report submitted to the Engineering Management Program  
and the Faculty of the Graduate School of The University of Kansas in partial  
fulfillment of the requirements of the degree of the Master of Science.**

---

**Chick Keller**  
**Date**  
**Committee Chair**

---

**Herb Tuttle**  
**Date**  
**Committee Member**

---

**Annette Tetmeyer**  
**Date**  
**Committee Member**

## **Acknowledgements**

I would like to thank my parents who have always been very supportive of my career as well as my education.

I personally would like to thank Prof. Chick Keller and Annette Tetmeyer for giving me great guidance and advice on my field project. I especially would like to thank Prof. Herb Tuttle for looking after my field project progress as well as supporting me on this project. I also would like to thank the NTS division of the University of Kansas for providing me a great deal of useful information on the wireless security issues on campus.

## Table of Contents

Acknowledgements.....	2
Executive Summary.....	5
Purpose.....	7
Introduction.....	8
Wireless Threats .....	11
Literature Review.....	13
Process and Methodology.....	21
Development of Survey .....	22
Development of Interview .....	24
Summary and Conclusion.....	27
Key Findings from the Survey.....	27
SWOT Analysis .....	31
Conclusion .....	34
Suggestions for Additional Work .....	36
Lessons Learned.....	36
References.....	37
Appendix A – Glossary of Terms .....	38
Appendix B – Acronyms and Abbreviations.....	41
Appendix C – Information Privacy and Security Awareness Survey.....	43
Appendix D – Raw Data Obtained from the Survey .....	45
Appendix E – Statistical Calculations.....	50

## List of Figures

Figure 1: Wireless Data Network Protected by WPA and VPN Security Solutions .....	10
Figure 2: General Classification of Wireless Attacks.....	11
Figure 3: Win Sniffer .....	12
Figure 4: Network Topology with VPN and WPA Support Elements .....	15
Figure 5: VPN Technologies and the OSI Model.....	19
Figure 6: Illustration of the security wheel technique commonly used as a tool to craft a security policy.....	20
Figure 7: The Importance Level of Wireless Security on Campus.....	27
Figure 8: User Concern about Wireless Threats .....	28
Figure 9: User Knowledge of Self-Defense against Wireless Threats .....	29
Figure 10: User Preference for Wireless Security Solutions .....	30
Figure 11: Brief Results of the SWOT analysis.....	31

## List of Tables

Table 1: Types of Network Attacks.....	8
Table 2: Security Features Provided in Each Wireless Standard.....	14
Table 3: General Characteristics of the Given Network Types .....	29
Table 4: Strengths of the WPA and VPN Security Solutions.....	32
Table 5: Weaknesses of the WPA and VPN Security Solutions .....	33
Table 6: Opportunities of the WPA and VPN Security Solutions .....	33
Table 7: Threats to the WPA and VPN Security Solutions .....	34

## **Executive Summary**

Many university information services departments have been gradually extending their wireless local area network (WLAN) coverage in order to provide wireless access to students, staff, and faculty throughout their campuses. There is a growing concern about security risks inherent with a wireless data network, such as loss of confidentiality, loss of integrity and loss of network availability (Karygiannis & Owens, 2002). According to a number of studies, the traditional wireless security services, based on the IEEE 802.11 standard as known as Wired Equivalent Protection (WEP) and commonly used in university's wireless data networks, are hopelessly flawed and have failed to provide a robust security system to a wireless network (Sankar, Sandaralingam, Miller, & Balinsky, 2004).

Designing a wireless security service for a university environment requires more comprehensive understanding than that for a public place, home, organization, or governmental office. The wireless data network of a university has to be very flexible so that it can support a variety of user behaviors from a number of different types of wireless terminals like in an open public place. In addition, the wireless data network must be capable of efficiently authenticating a user to an access point (AP) and vice versa, and to ensure that the user's information and data being propagated in the air are secure. Thus, deploying a wireless network security based on the Wireless Protected Access (WPA) specification with Virtual Private Network (VPN) technology should be the most appropriate solution to effectively securing a university's wireless data network.

With the WPA and VPN security solutions, a university information services (IS) department will be able to satisfy the user needs by providing a strong wireless security

to its users and supporting all types of wireless devices. In addition, the university IS department can increase its wireless data network performance by utilizing existing network elements, such as wireless APs and VPN equipment, and improving its network services, operation and management. And at the very least, while providing sufficient security based on WPA and VPN security solutions to its users, the university IS department can lower the network installation costs and thoroughly work on a smooth transition to the wireless security service based on the IEEE 802.11i standard, which is expected to be widely implemented in the future (Perez, 2004).

## **Purpose**

This field project is intended to determine that there is a need to improve the wireless network security on campus. Universities need to be attentive to the security issues and the user needs of secure wireless services on campus as there are potential threats in a wireless data network. Consequently, the author proposed the WPA and VPN technologies as the most effective solution in a university environment that brings a number of advantages to both universities and their wireless users.

The author first addressed the severe security weaknesses of a wireless data network protected by the ordinary 802.11 WEP security scheme, and the advantages of deploying WPA together with the VPN technology in a university's wireless data network. The author then used a survey technique to collection information from users in order to draw a conclusion on the user needs of wireless security services on campus. On the other hand, an interview approach was used to gather data regarding security issues and managerial aspects of wireless security solutions. At the end, the author employed a SWOT analysis to summarize the findings from the research, survey and interview that lead to the conclusion of the proposed wireless security solution.

## Introduction

As wireless technologies advanced, many universities are utilizing as well as expanding their WLAN on campus as a tool that allows students, staff, and faculty members to access e-learning education, online accounts, BlackBoard, online libraries, and other helpful electronic resources available on the Internet anywhere on campus. Despite the advantages of a wireless data network in flexibility, efficiency, and network costs, there are great security risks that concern user confidentiality, data integrity, and network availability associated with any wireless data network (Karygiannis & Owens, 2002). According to the recent survey conducted by the Computer Security Institute (CSI) in 2006, 52 percent of the organizations polled stated that their network security defenses had been breached, and that 42 percent of the incidents came from their internal networks, costing \$1.85 million (Gordon, Loeb, Lucyshyn, & Richardson, 2006). **Table 1** shows the types of attacks, which are related to the network security issues, and their associated losses. Thus, a more efficient wireless security protection should be one of the primary concerns on which the IS department of a university has to focus so that all users and network elements can be safe from malicious attacks.

Type of Attack	Percentage	Loss (\$)
Insider Abuse of Net Access	42	1,849,810
Unauthorized Access to Information	32	10,617,000
Denial of Service	25	2,922,010
System Penetration	15	758,000
Abuse of Wireless Network	14	469,010
Theft of Proprietary Information	9	6,034,000
Sabotage of Data or Networks	3	260,000
TOTAL LOSS		22,909,830

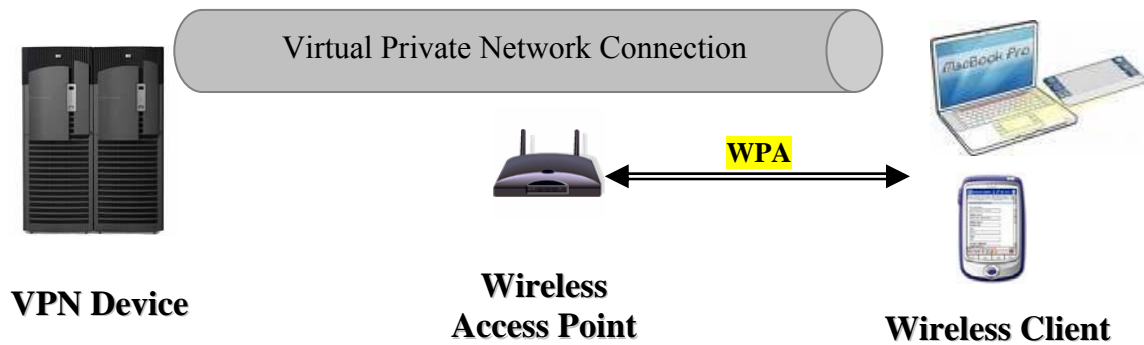
**Table 1: Types of Network Attacks**

Source: CSI/FBI Computer Crime and Security Survey (2006)



There are a number of standardized wireless security solutions available in the market as specified by IEEE 802.11 known as WEP (which is currently used in many universities' wireless data networks), WPA, IEEE 802.11i, and VPN. Apparently, each has different advantages and disadvantages in authentication as well as encryption mechanism. In spite of the fact that the WEP security standard supports a very wide range of wireless devices, it has a bad reputation for being relatively easy to crack, posing a large-scale threat to the users and wireless data network. On the other hand, 802.11i offers the highest security standard to the wireless data network as it enhances 802.11 with several new superior security mechanisms that address all of the confidentiality and integrity weaknesses of all previous specifications (Sankar *et al*, 2004). However, it requires a revolutionary change of both wireless AP and clients.

Regarding the certified wireless security professional study in 2003, WPA seems to have provided a relatively strong security protection to a wireless data network as it incorporates the advantages of the 802.1x technologies and some IP security mechanisms like the 802.11i specification, though, not as high as the 802.11i standard (Plannet3 Wireless, 2003). With the VPN technology implemented together with the WPA standard in a wireless data network as illustrated in **figure 1**, a university IS department can increase its wireless security services, satisfying the user needs with two choices of reliable wireless security options: WPA-based security for users who require a sufficiently secure wireless access, and VPN-based security for those who require a very secure wireless connection on campus.

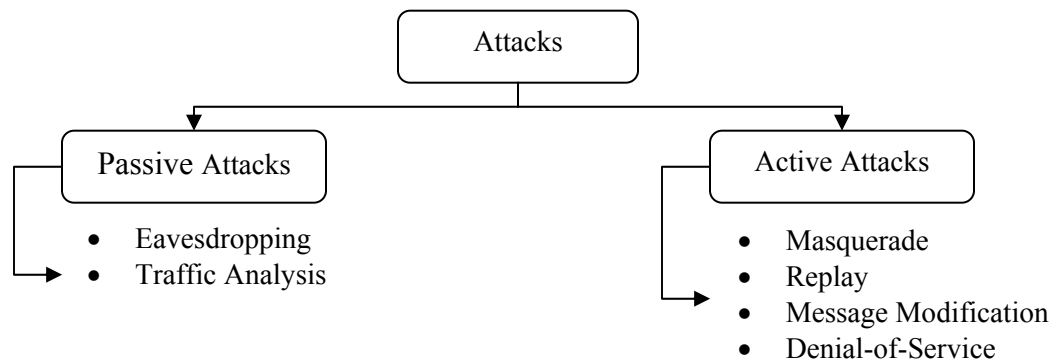


**Figure 1: Wireless Data Network Protected by WPA and VPN Security Solutions**

To design a wireless security solution for a university environment, one must thoroughly analyze the impact on both network infrastructure and clients due to the implementation while making an attempt to equip a wireless network with the most effective security protection. Unlike the 802.11i requirement, WPA can be implemented immediately and inexpensively as a software or firmware upgrade to the existing Wi-Fi CERTIFIED access points and client devices according to the Wi-Fi Alliance specifications (Sankar *et al*, 2004). That there will be no need to replace all of the existing wireless APs increases the utilization of the university's assets as well as lowering the network installation costs. In addition, a WPA-based wireless data network will continue to support all of its existing wireless devices. As a result, deploying the WPA and VPN technologies in a university's wireless data network will allow the university IS department to substantially improve its network performance in terms of network utilization, and network operation and management.

## Wireless Threats

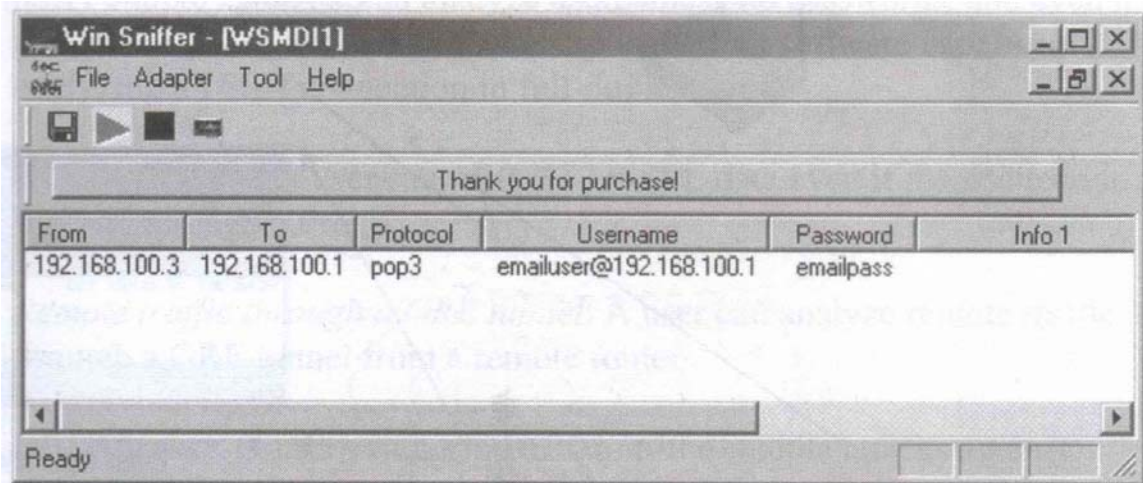
As wireless technologies rapidly advance, malicious tech-savvy thieves have also quickly developed their notorious attack skills on a wireless data network and people who are using it. In an insecure or inadequately secure wireless data network environment, they can simply cause serious risks to security, for example, loss of confidentiality, loss of integrity, loss of network service, legal and recovery costs, and tarnished image (Karygiannis *et al*, 2002). In general, attacks on a wireless data network are divided into two board classes: passive and active attacks. **Figure 2** provides a classification chart of wireless attacks against WLANs.



**Figure 2: General Classification of Wireless Attacks**

Source: Karygiannis, T., & Owens, L. (2002). *Wireless Network Security: 802.11, Bluetooth and Handheld Devices* (Special Publication 800-48)

A passive attack occurs when an unauthorized party monitors or eavesdrops on network traffic without modifying its contents, compromising the confidentiality of sensitive or proprietary information of the wireless network users (Nichols & Lekkas, 2002). Examples of eavesdropping and traffic analysis are War Driving and WiPhishing. **Figure 3** illustrates a data sniffing application named Win Sniffer which is capable of decrypting email passwords from the user information sent in the air.



**Figure 3: Win Sniffer**

Source: Planet3 Wireless Inc. (2003). *CWSP Certified Wireless Security Professional Official Study Guide (Exam PW0-200)*.

The other type of attack on a wireless data network is the active attack. Unlike the passive attack, an unauthorized party makes modifications to a message and file of the wireless users as well as sabotaging the data network and wireless devices (Karygiannis *et al*, 2002). This type of wireless security threat basically compromises data integrity, network availability, and user confidentiality.

There are a number of ways a malicious intruder can commit an active attack. Masquerading as an authorized user is the most common example by which an attacker can gain certain unauthorized privileges of a wireless data network (Karygiannis *et al*, 2002). The most common techniques that most intruders use are breaking the client's authentications and masquerading as a legitimate wireless access point to the wireless clients. Once the necessary information has been obtained, they can now access the network elements or wireless terminals and cause all kinds of damages to them.

## **Literature Review**

Sankar, K., Sandaralingam, S., Miller, D., & Balinsky, A. (2004). *Cisco Wireless LAN Security*. Indianapolis, IN: Cisco Press.

Despite its quick deployment and full compatibility with all existing network elements, the WEP security scheme is seriously flawed which many tools available in the market can readily exploit some of these flaws. WEP employs the RC4 encryption algorithm that inadequately encodes a message with either a 40-bit or 104-bit key for the purpose of data integrity and confidentiality. As a result, an attacker with a publicly available WEP cracking tool, such as AirSnort and AirCrack, can most likely decrypt the message in a matter of minutes. Other common types of wireless threats are reconnaissance attacks, DoS attacks, authentication attacks, and WEP key stream and plaintext recovery.

WPA came out in 2003 as an intermediate solution to the security pitfalls before the introduction of the IEEE 802.11i standard. Both WPA and IEEE 802.11i are designed to eliminate the problems resulted from the authentication and encryption weaknesses of WEP. The major improvement in WPA over WEP in terms of security issues is the use of TKIP with RC4 in encryption algorithm along with EAP for authentication. Not only does TKIP fix the problem encryption of WEP, it was designed to work with legacy hardware already deployed in wireless data networks, for example, network interface cards and access points.

IEEE 802.11i is the standard that specifies security mechanisms used in wireless data networks. Other than using EAP for authentication, IEEE 802.11i also makes use of the AES-based CCMP technique to strengthen data confidentiality and integrity.

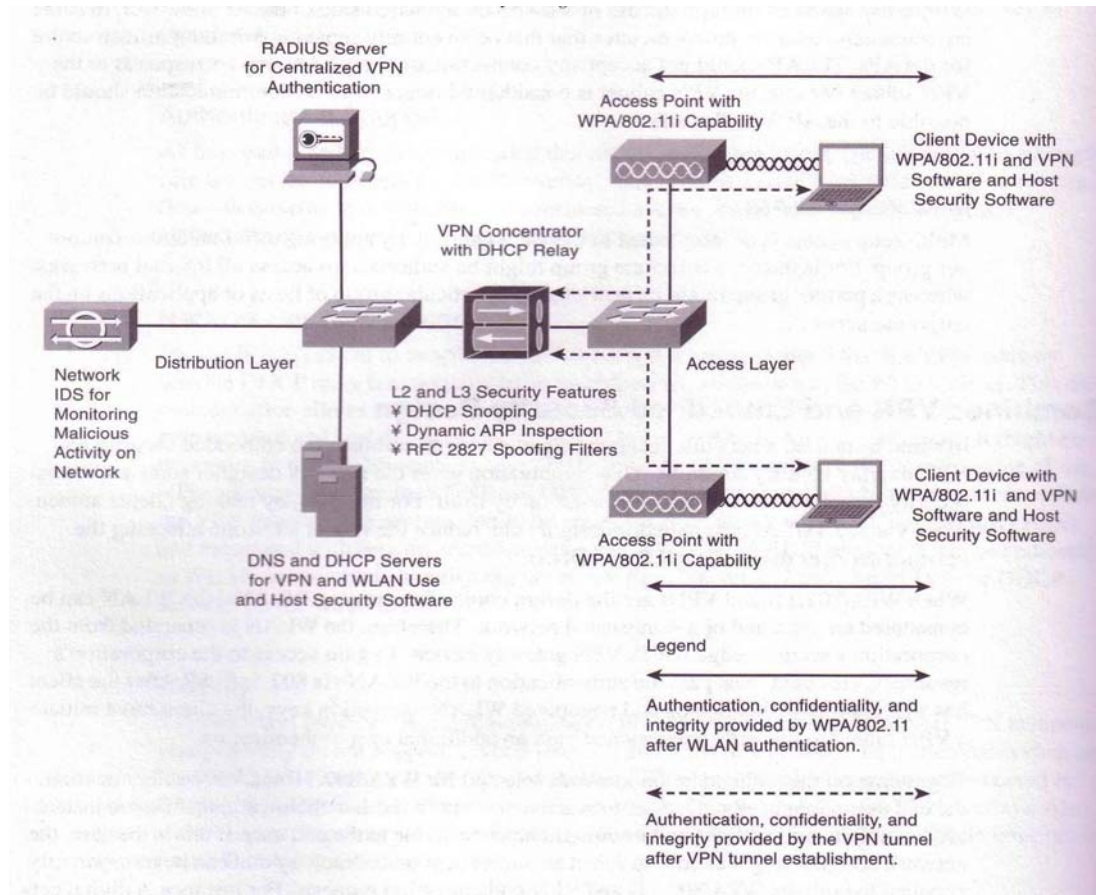
Although capable of providing stronger encryption and message integrity than WPA, IEEE 802.11i is not fully compatible with the WEP-based hardware.

FEATURE	802.11 / WEP	WPA	802.11i
Authentication	Shared key/EAP	UN/PW (with RADIUS), Shared key, Protected EAP	UN/PW (w/ RADIUS) Protected EAP
Integrity	32-bit Integrity Check Value	64-bit Message Integrity Code	CCM
Encryption	Static keys	Key rotation using TKIP	CCMP
Evolutionary / revolutionary		Evolutionary	Revolutionary

**Table 2: Security Features Provided in Each Wireless Standard**

Source: Sankar, K., Sandaralingam, S., Miller, D., & Balinsky, A. (2004). *Cisco Wireless LAN Security*.

Designing a secure, cost-effective wireless data network is a challenge task for any network designer and administrator. They need to understand how to simultaneously support existing WLAN architecture and introduce the new security technology to the network. The implementation of VPN on top of WPA security design is a solution that requires a slight software upgrade in network elements and users due to the WPA specification. **Figure 2** illustrates the security solution of implementing the VPN technology to a wireless data network already protected by the WPA security scheme. In the meantime, the network can be far more secure as the VPN security solution eliminates many of the possible threats inherent with WPA encryption mechanism.



**Figure 4: Network Topology with VPN and WPA Support Elements**

Source: Sankar, K., Sandaralingam, S., Miller, D., & Balinsky, A. (2004). *Cisco Wireless LAN Security*.

Planet3 Wireless Inc. (2003). *CWSP Certified Wireless Security Professional Official Study Guide (Exam PW0-200)*. Emeryville, CA: McGraw-Hill/Osborne Media.

With decent wireless hacking tools simply found on internet, malicious intruders can most definitely obtain users' information transmitted in a wireless data network based on the WEP security scheme, which is part of the ordinary IEEE 802.11 specifications. Besides, they can easily cause a serious security breach as well as posing several DoS attacks to the network. According to many studies, there are a number of weaknesses found in WEP, leaving both users and networks vulnerably exposed to serious threats, for instance, forgery, weak-key attacks, collision attacks, and replay attacks.

After WEP has been proved ineffective to secure a wireless computer network, the Wi-Fi Alliance introduced WPA in 2003, addressing the weaknesses of WEP with a minor change in the network. WPA provides stronger data encryption through Temporal Key Integrity Protocol (TKIP) and mutual authentication through the Extensible Authentication Protocol (EAP) of the IEEE 802.1x standard. However, it could not provide the highest data security protection because of the hardware restraints of the existing network elements.

IEEE 802.11i is the latest standard ratified on June 25, 2004, offering the most sophisticated security mechanisms that eliminate all pitfalls of both WEP and WPA. It employs multiple methods of using Advanced Encryption Standard (AES) as its underlying security technology. Consequently, implementing the IEEE 802.11i standard as a security solution will require a major change in the wireless network elements and wireless terminals due to the cryptographic overhead of AES.

Gast, M. S. (2002). *802.11 Wireless Networks: The Definitive Guide*. Sebastopol, CA: O'Reilly & Associates, Inc.

WEP is so flawed that it is unable to protect a wireless data network from malicious attacks. The major problem of WEP is caused by the severe design flaws. The technical issues regarding the design flaws are the network's WEP keys, the inadequacy of its encryption bits, the stream ciphers infrequent rekeying of WEP, and its use of CRC for the integrity check.

In August 2001, there was a paper "Weaknesses in the Key Scheduling Algorithm of RC4" by Scott Fluhrer, Itsik Mantin, and Adi Shamir describing a theoretical attack



that leads to the complete break of WEP. The root cause of all WEP security problems was the result of its cryptographic cipher – the key scheduling algorithm of RC4.

Yuan, R. & Strayer, W. T. (2001). *Virtual Private Networks: Technologies and Solutions*. Boston, MA: Addison-Wesley Professional.

The main purpose of VPN technologies is to allow an authorized network access from other networks while providing strong data integrity and confidentiality to users and clients. A VPN gateway is the primary network element that provides a virtual, secure connection between the users or clients and servers. VPN tunneling protocols and cryptographic algorithms are fundamentally employed to ensure that data security is not compromised and that the encrypted message being transmitted can be read only by the intended recipients. VPNs also use a digital signature process to authenticate the authorship of a message. As a matter of fact, the digital signature is analogous to a handwritten signature of the person who has sent the message. Moreover, the network elements use it as a means to verify whether or not the message received has been altered or distorted during the transmission.

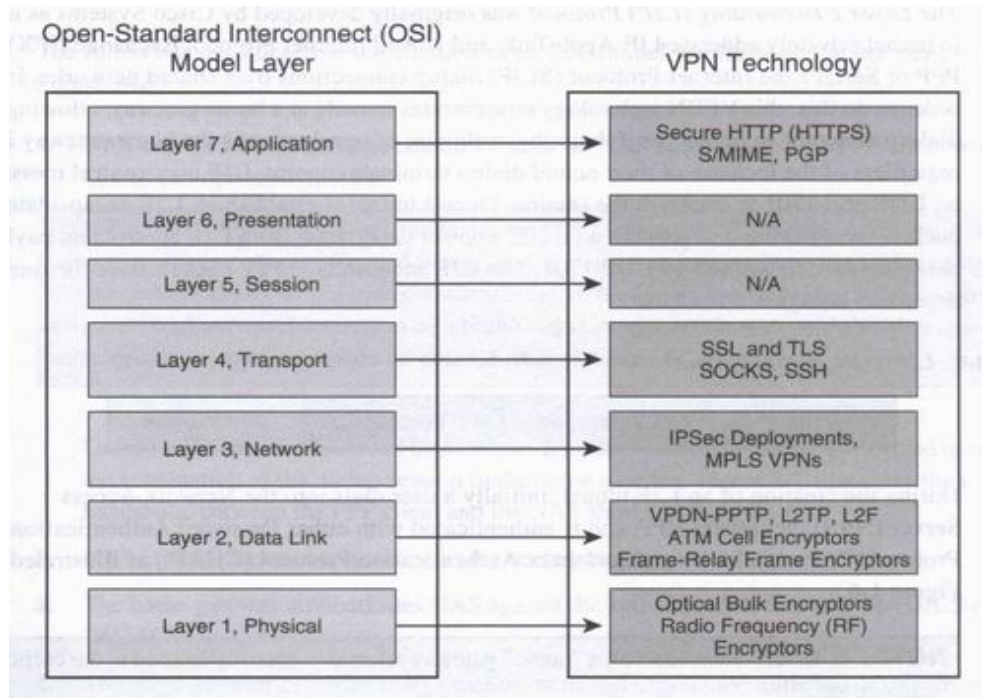
Other than providing superior network security features to data networks, implementing the VPN solution to a corporate data network allows the IT department to minimize the costs associated with the data security protection of the company. The VPN solution makes it possible for any organization to build a secure, cost-effective connection on top of its existing vast, shared, and unsecured infrastructure which is mostly based on internet. The IT department will not have to provide any additional

private link when there are new database servers, clients, or network topology changes. Thus the costs of network implementation can be reduced.

Carmouche, J. H. (2006). *IPsec Virtual Private Network Fundamentals*. Indianapolis, IN: Cisco Press.

There is a need for securing data that traverses a wireless data network. VPN technologies are the solution that allows the data to be securely and privately transmitted data over an insecure, shared data network while greatly reducing IT operational expenditures.

The two primary methods deployed by VPN technologies are encapsulation and encryption. Basically, they increase data confidentiality by protecting the information transmitted in the data network from being read by intruders. Moreover, they ensure and guarantee that a message sent and received is authentic and without any alteration in transit. Another outstanding characteristic of the VPN technology is sender non-repudiation, which prevents senders from deliberately denying that they have transmitted the message to the receiving party.



**Figure 5: VPN Technologies and the OSI Model**

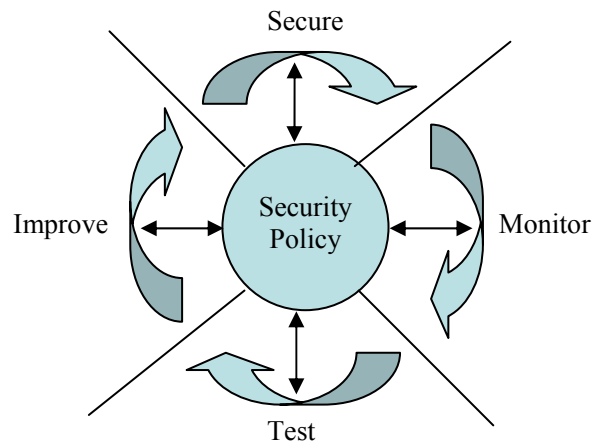
Source: Carmouche, J. H. (2006). *IPsec Virtual Private Network Fundamentals*.

Technically speaking, VPNs have been designed to protect data at many layers; ranging from Layer 1 with bulk encryptors to Layer 7 with secure HTTP. As shown in **figure 2**, there are a number of VPN security solutions that a network designer may consider deploying together with WPA. With the deployment of VPN technologies, an organization will be able to enhance the flexibility of its network, increasing the efficiency of the business communications.

Mason, A. G. (2004). *CCSP Self-Study: Cisco Secure Virtual Private Networks (CSVPN) (2<sup>nd</sup> ed.)*. Indianapolis, IN: Cisco Press.

It is imperative that a continuous security policy be effectively implemented in an organization. The information services department of an organization needs to develop a

security policy that addresses security measures necessary for securing its network infrastructure.



**Figure 6: Illustration of the security wheel technique commonly used as a tool to craft a security policy.**

Source: Mason, A. G. (2004). *CCSP Self-Study: Cisco Secure Virtual Private Networks (CSVPN)* (2<sup>nd</sup> ed.).

For an organization that uses a shared public network infrastructure as a means of communications, a VPN can definitely offer secure, reliable services for data transmission. It simply increases security and reliability of the network with its sophisticated tunneling protocols and encryption software. Increasingly, the VPN technology has been widely implemented wireless data networks in order to maximize confidentiality, data integrity, and authentication levels, ensuring complete privacy of the data propagated in sure shared, vulnerable transmission medium.

In addition, with the VPN security solution, organizations can effectively lower their costs of installing expensive private connections and telephone systems. The VPN technology can be easily implemented to an existing data network. The network administrator will find it very flexible and scalable to manage both now and in the future.

## **Process and Methodology**

Being able to understand and provide what the users or customers want is one of the key success factors of implementing changes into an organization. Likewise, a new wireless security implementation on campus will likely be successful if the university IS department can satisfy the user's needs. There are many techniques that can be deployed to acquire an in-depth understanding about the user's perspective on the security protection of a wireless data network on campus. Apparently, a survey is a cost-effective means to collect comprehensive data from a large number of respondents in a university environment. Thus, the author chose a researcher-administered survey as an approach to drawing a conclusion on the user needs of the wireless security issues in a university environment.

While the survey had been deployed to gather data from network users, the author used an interview technique to gather accurate information about the wireless security issues on campus from those who have considerable expertise in a university's wireless data network operation and management. Their insight about the wireless security solution on campus will allow the author to gain full range and depth of information necessary for building SWOT analysis of the proposed wireless security solution.

A SWOT analysis is an excellent tool in crafting a good strategic plan, allowing an organization to understand its current status (Keller, 2005). Accordingly, the SWOT analysis was used to address both internal (strengths and weaknesses) and external (opportunities and threats) factors of implementing the WPA and VPN security solution to a university's wireless data network. After having analyzed the data obtained from the

survey and interview, the author was able to create **tables 4, 5, 6, and 7** in the next section as the results of a SWOT analysis.

## **Development of Survey**

The survey was entitled “Information Privacy and Security Awareness” developed to provide a snapshot of the wireless network users’ sense of security in their personal confidentiality on a university campus. The author was also hoping that the survey would raise security awareness among the people who are using wireless data network services on campus.

## **Questions**

The questionnaire was carefully crafted to discover the users’ awareness and concerns about the security issues of a wireless data network as well as the overall characteristics of a secure wireless data network they are looking for. The author first incorporated an example of the threats inherent with the wireless communication technology as the introductory part of the survey. In addition, to give a better understanding to the respondents about potential threats in a wireless data network, some common examples of how a malicious intruder can attack them and their wireless devices were included in the survey.

Although incorporating some knowledge about the wireless threats into the survey may seem to make the data from the survey become biased, it is imperative that the respondents have a good understanding before expressing their opinions. Therefore, educating the respondents is an approach to gather the most accurate information on how the wireless users respond to the security issues of a wireless data network on campus.

The survey comprises four questions relating to the security issues on which respondents were asked express their opinions. Those questions are categorized into three areas of interest as follows:

*Security Awareness*

- 1) How important the respondents think the security of the wireless data network should be.
- 2) How much the respondents are concerned about the threats that possibly come from a wireless data network they are using.

*Security Protection Knowledge*

- 3) How much the respondents know about protecting themselves and their wireless devices from the wireless attacks.

*User Preference*

- 4) The general characteristics of a secure, reliable wireless data network that the respondents wish to see in place.

**Survey Methodology**

The author targeted at those who were using their wireless terminals, such as laptops and PDAs, to access the Internet or intranet through the wireless data network services of a university. The survey was administered to the wireless users between 11 AM and 2 PM at libraries and cafeterias on a university campus. To lessen the bias from the survey, the author conducted the survey for four days (Monday to Thursday) at the same period of time and locations, and with the same number of samples (30 samples on each day). Shown in **appendix D**, the raw data collected from the survey was processed

statistically and presented in graphics. **Appendix E** illustrates how the confidence level and the sampling error of the survey had been calculated. The survey findings are shown and discussed in greater detail in the next section – Process and Methodology.

## **Development of Interview**

The author used an interview approach to gather accurate information about the wireless security issues on campus from those who have considerable expertise in a university's wireless data network operation and management. Their insight about the wireless security solution on campus will allow the author to gain full range and depth of information necessary for building SWOT analysis of the proposed wireless security solution.

### **Selecting the Interviewees and Directing the Questions**

The interviewees were chosen from three distinct domains of a university's wireless data network: network director, network architect, and network operator. In order to obtain the most relevant and comprehensive knowledge about wireless security solution, the questions directed to them were somewhat different.

During the interview with the network director, the author focused mostly on the managerial issues of how the computer network services unit of the subject university meets the information technology needs of wireless users on campus while maintaining user privacy and the security measures of its wireless data network. The main questions raised from the research were:



- 1) What is the current security policy on the university's wireless data network on campus and the current security protection?
- 2) What are the strengths, weaknesses, opportunities and threats of the current wireless security protection?
- 3) What is the new or long-term solution to the problems or security threats?
- 4) What are the concerns about the new solution and expectations of it and how would it affect the users – students, staff and faculty on campus?

The network architect was also interviewed with the same set of questions used at the interview with the network director. However, the author particularly focused on the concerns regarding how to design and implement a wireless security that will cause minimum impact on network users and network operation and management. The issues on the network utilization and wireless network security technologies were also discussed in detail during the interview.

The key questions directed to the network operator were structured to gather the information about the most effective way in which a university's wireless data network should be securely operated. Those questions are as follows:

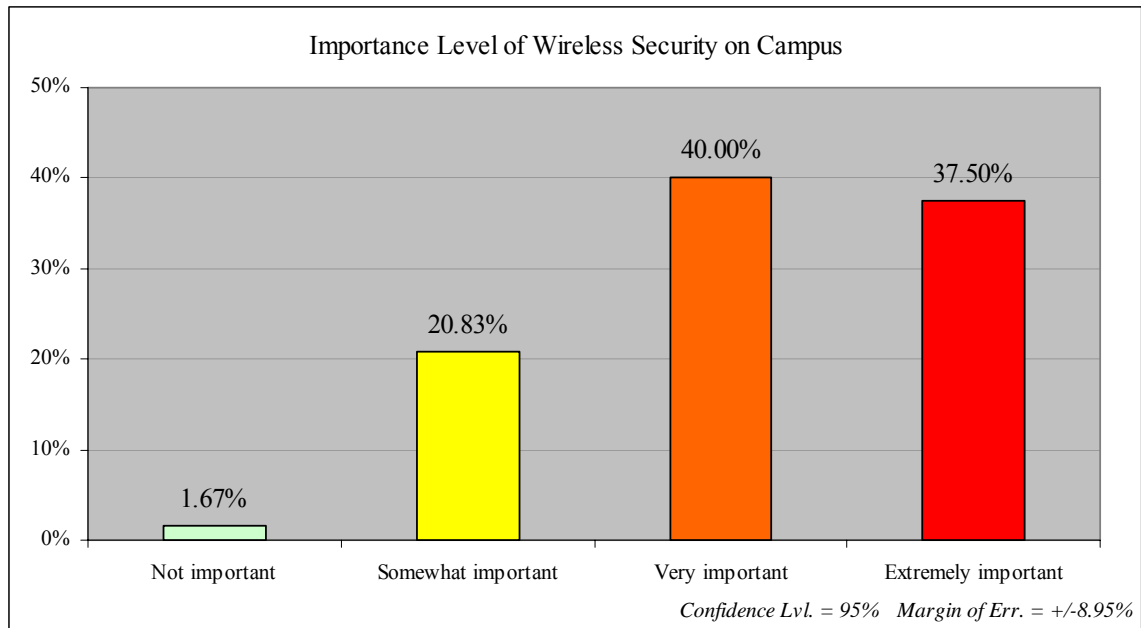
- 1) How does the computer network services unit implement a wireless security solution to the entire university's data network?
- 2) What are the problems or obstacles to the computer network services unit managing the wireless security policy?
- 3) What are the advantages and disadvantages of the new security solution in terms of network operation and management?

- 4) What are the concerns about the new security solution and expectations of it and how would it affect the users – students, staff and faculty on campus?

## Summary and Conclusion

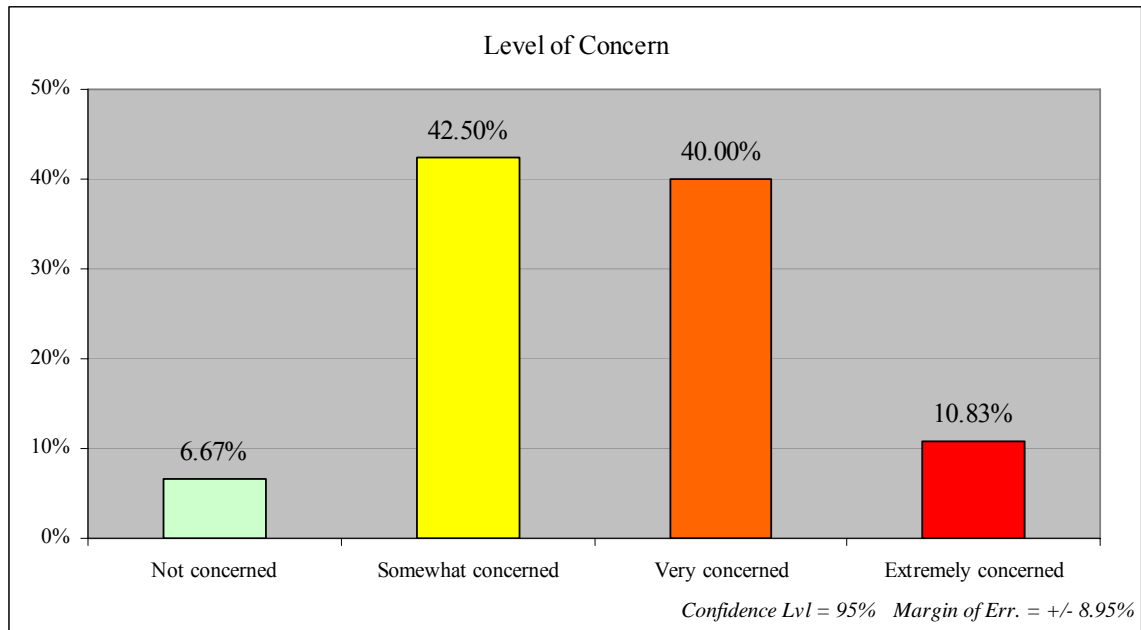
### Key Findings from the Survey

The survey was conducted between 11 AM and 2 PM from March 5<sup>th</sup> to March 8<sup>th</sup>, 2007 and was administered to 120 wireless network users on campus. Shown in **appendix D**, the raw data obtained from the survey was statistically processed by Microsoft Excel and the results of the survey are expressed in the following graphs:



**Figure 7: The Importance Level of Wireless Security on Campus**

As the network users' daily activities involve many applications based on wireless internet access on campus, the wireless security issue seems to have played a vital role in a university's wireless data network. The great majority of the network users on campus, 77.50% as shown in **figure 7**, view that it is very or extremely important to have a wireless security measure in place.



**Figure 8: User Concern about Wireless Threats**

As wireless internet access has dramatically brought more benefits to students, staff and faculty on campus, there is a considerable amount of concern about wireless threats that also come along with the wireless data network. According to **figure 8**, 50.83% of the wireless network users on campus are very or extremely concerned about the wireless threats.

When asked about their knowledge level of protecting themselves and their wireless terminals from being attacked by wireless attackers, 25.83% of the respondents either do not know or knew a little about self-defense against wireless threats. For an insecure wireless data network, any information sent between wireless terminals and network access points can be intercepted and read easily by any wireless cracking tool with adequate computing power. As a result, those 38.33% of the respondents who expressed good or excellent knowledge of protecting themselves from such threats from the survey may also be as vulnerable as others. **Figure 9** illustrates five groups of

wireless network users who possess different knowledge level of self-defense against malicious wireless attacks.

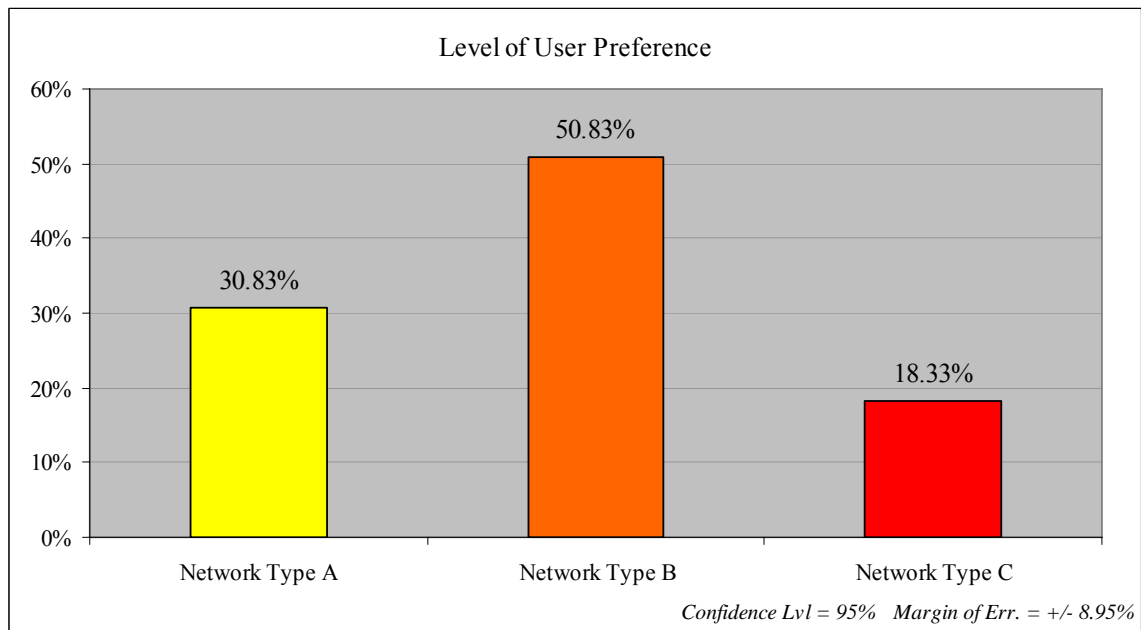


**Figure 9: User Knowledge of Self-Defense against Wireless Threats**

Choice	Characteristics	Wireless Security Solution
Network A	Low security protection. Very easy to access (only user name and password required)	802.11 / WEP
Network B	High security protection. Initial security setup required. Software and/or firmware upgrade may be required.	WPA
Network C	Very high security protection. Initial security setup required. Software and/or firmware upgrade may be required. Some wireless terminals, such as PDAs and laptops with old operating system, are no longer supported by this type of wireless data network	802.11i

**Table 3: General Characteristics of the Given Network Types**

In addition to gathering information on the user security awareness issues, the survey also asked the wireless network users to choose which network type they prefer. Three choices were provided in the survey, briefly describing general characteristics of the three well-known wireless security solutions as shown in **table 3**.

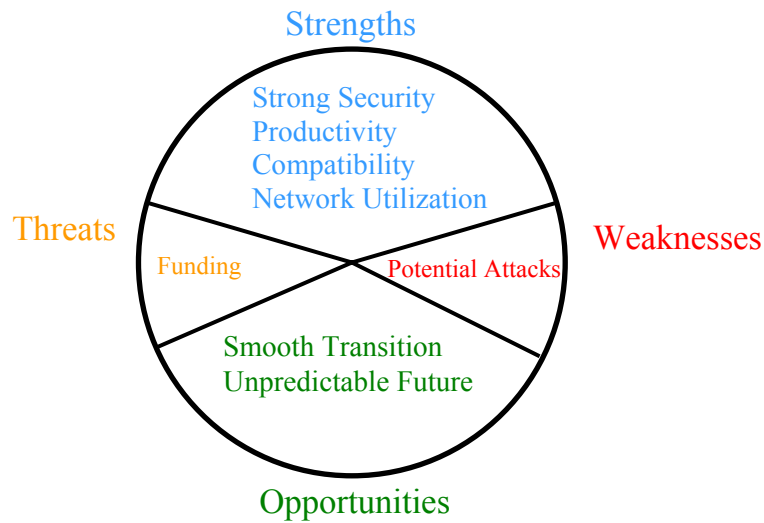


**Figure 10: User Preference for Wireless Security Solutions**

A majority of the respondents, 50.83% as indicated in **figure 10**, preferred the network type B, a wireless data network protected with the WPA wireless security solution. On the other hand, only 18.33% of the wireless users would want to see the wireless data network on campus equipped with the most sophisticated 802.11i wireless security solution. Thus, the most obvious, interesting finding is that the users do not wish to see their wireless data network on campus offer the strongest security protection while unnecessarily rendering some of their old wireless terminals obsolete.

## SWOT Analysis

After analyzing the information obtained from both the survey and interview approaches, the author was able to perform a SWOT analysis on the WPA and VPN security solutions. **Figure 11** illustrates the concise results of the SWOT analysis. The detailed descriptions of the strengths, weaknesses, opportunities, and threats of the proposed solution are tabulated in **tables 4, 5, 6, and 7**, respectively.



**Figure 11: Brief Results of the SWOT analysis**

### ***Strengths***

<b>Issue</b>	<b>Description</b>
Strong Security Protection	The WPA security scheme sufficiently serves as a fundamental security protection in a wireless data network. The VPN technology implemented over a WPA-based wireless data network will provide a very secure wireless connection for those who need it on campus.
Relatively Low Network Installation Costs	When compared with the 802.11i security solution, a university IS department can lower the costs of new network equipment and installation.
Higher Utilization of Existing Data Network Equipment	A university IS department will still be able to use some of the existing wireless access points. In addition, it can also take more advantage of its existing VPN network.
Increase in User Confidence and Productivity	Students, staff, and faculty members can be more confident of using wireless internet access anywhere on campus. Thus, time can be saved and more work can be completed.
User Wireless Terminal Compatibility	Unlike the 802.11i design restraint, a WPA-based wireless data network will be able to support those old, existing wireless terminals of the users on campus.
Ease of Wireless Data Network Operation and Management	With more features and options that come with the new data network equipment, especially backbone machines, a university IS department will be able to improve its network scalability, granularity in administration.

**Table 4: Strengths of the WPA and VPN Security Solutions**



### *Weaknesses*

<b>Issue</b>	<b>Description</b>
Relatively High Core Data Network Investment	When compared to the WEP security solution, there is a considerable amount of network investment depending on the coverage of a wireless data network on campus.
Potential Security Threats	As the VPN connection is an optional service to users, those who rely only on the fundamental security service offered by the WPA security solution are still vulnerable to some highly skillful wireless intruders.

**Table 5: Weaknesses of the WPA and VPN Security Solutions**

### *Opportunities*

<b>Issue</b>	<b>Description</b>
Road Map to 802.11i-based Wireless Data Network	There have not been any reports or studies of the cost-benefits analysis or the efficiency of an 802.11i-based wireless data network on campus. Perhaps, it is better for a university IS department to deploy the WPA and VPN security solutions as an intermediate plan before implementing complete 802.11i security services to the entire network.
Unpredictable Future Threats	The 802.11i standard may not always remain unbreakable as technologies rapidly change. Thus, it may eventually leave the wireless network users as vulnerable as both WEP and WPA do in the near future.
Minimum Impact on Users	While operating the WPA and VPN security solutions, a university IS department can conduct a comprehensive research on how the 802.11i security solution would affect the wireless network users. Thus, the negative impacts from the 802.11i security solution on the end users can be mitigated or eliminated in advance.

**Table 6: Opportunities of the WPA and VPN Security Solutions**

### ***Threats***

<b>Issue</b>	<b>Description</b>
Funding	Due to the considerable amount of network investment, tight university budgets may limit the complete solution of WPA combined with the VPN technology.
Potential Security Threats	As the VPN connection is an optional service to users, those who rely only on the fundamental security service offered by the WPA solution are still vulnerable to some highly skillful wireless intruders.

**Table 7: Threats to the WPA and VPN Security Solutions**

### **Conclusion**

Wireless access services on a university campus offer students, staff, and faculty numerous benefits, such as mobility, increased productivity, and lower data network investment. As wireless technologies rapidly advance, malicious tech-savvy thieves become more skillfully cunning. The result of the survey clearly prove that wireless network users on campus are concerned about several types and sizes of wireless threats lurking both outside and inside of the university's wireless data network they are using. Consequently, the university IS departments should be attentive to the security needs of their users, making their wireless data networks secure and continuously updating their wireless security measures and policies.

To maintain the security of a university's wireless data network and user privacy, security issues have to be addressed at all levels: network users, network elements, technologies, applications, network administrators, and policies. Considering the security issues on the interface between users and the wireless data network, there are a few standardized technologies available in the market that an organization can employ to

secure such interfaces. However, the author focused on a wireless security solution based on WPA and VPN technologies which prove to have satisfied the security needs of the users.

As in a university environment, a majority of users realize the importance of the wireless security. They are concerned about all kinds of potential wireless threats, but still want to keep using their old wireless terminals. Moreover, many of them do not possess adequate knowledge of protecting themselves against those threats.

With WPA security features implemented in its wireless data network, a university IS department will be able to provide sufficient security services to a variety of wireless clients and devices. In addition, with the VPN technology the university can offer a much stronger secure wireless connection to those who consider their confidentiality extremely critical. In the meantime, the university IS department can work on a smooth transition to the 802.11i-based wireless data network without unnecessarily investing a great amount of money all at once.

In conclusion, deploying WPA together with the VPN technology is the most effective wireless network security solution in a university environment. Thus, the universities should consider the WPA standard as a fundamental wireless security protection and the VPN technology as an add-on service for a stronger wireless security protection on campus. The WPA and VPN security technologies are also a viable wireless security solution for those universities that are somewhat uncertain about the wireless technologies and threats in the future.

## **Suggestions for Additional Work**

Rogue access point is an interesting security issue that has gradually become a significant threat to the wireless users on campus. There is no wireless security solution mentioned in this paper that can completely eliminate this type of problem. Educating wireless users about potential threats of a rogue access point seems to be the most effective solution to such security threats. At the same time, the university IS department should develop and deploy a technology solution that can best solve the rogue access point problem. A survey approach with comprehensive questions related to rogue access point can be performed to gather information for the research.

## **Lessons Learned**

The most interesting lesson that the author learned from this field project is that management has to understand and deliver what the users or customers really want. Therefore, it is imperative that management has to recognize the user needs as part of the project objectives and specifications.

## References

- Carmouche, J. H. (2006). *IPsec Virtual Private Network Fundamentals*. Indianapolis, IN: Cisco Press.
- Gast, M. S. (2002). *802.11 Wireless Networks: The Definitive Guide*. Sebastopol, CA: O'Reilly & Associates, Inc.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *CSI/FBI Computer Crime and Security Survey (2006 Survey)*. San Francisco, CA: Computer Security Institute (CSI).
- Karygiannis, T., & Owens, L. (2002). *Wireless Network Security: 802.11, Bluetooth and Handheld Devices* (Special Publication 800-48). Gaithersburg, MD: National Institute of Standards and Technology (NIST).
- Keller, C. W. (2005, Fall). *Strategic Analysis of Technological Project*. EMGT821: The University of Kansas.
- Mason, A. G. (2004). *CCSP Self-Study: Cisco Secure Virtual Private Networks (CSVPN) (2<sup>nd</sup> ed.)*. Indianapolis, IN: Cisco Press.
- Nichols, R. K., & Lekkas, P. C. (2002). *Wireless Security: Models, Threats, and Solutions*. McGraw-Hill TELECOM Professional.
- Perez, E. (2004). *802.11i (How We Got Here and Where Are We Headed)*. Retrieved December 20, 2006, from SANS Institute Web site:  
[http://www.sans.org/reading\\_room/whitepapers/wireless/1467.php](http://www.sans.org/reading_room/whitepapers/wireless/1467.php)
- Planet3 Wireless Inc. (2003). *CWSP Certified Wireless Security Professional Official Study Guide (Exam PW0-200)*. Emeryville, CA: McGraw-Hill/Osborne Media.
- Sankar, K., Sandaralingam, S., Miller, D., & Balinsky, A. (2004). *Cisco Wireless LAN Security*. Indianapolis, IN: Cisco Press.
- Yuan, R. & Strayer, W. T. (2001). *Virtual Private Networks: Technologies and Solutions*. Boston, MA: Addison-Wesley Professional.

## **Appendix A – Glossary of Terms**

Advanced Encryption Standard (AES)	An encryption algorithm for securing sensitive but unclassified material by the U.S. government agencies.
Access Point (AP)	A device that connects wireless communication devices together to form a wireless network.
Asynchronous Transfer Mode (ATM)	A cell relay, circuit switching network and data link layer protocol that encode data traffic into small fixed-sized cells.
Counter with Cipher Block Chaining Message Authentication Code (CCM)	Short for CRT/CBC-MAC, a mode of AES that combines CTR and CBC-MAC and achieves both confidentiality and integrity.
Counter Mode with CBC-MAC Protocol (CCMP)	Short for CRT/CBC-MAC Protocol, an IEEE 802.11i encryption protocol that uses the AES algorithm.
Computer Security Institute (CSI)	A professional membership organization serving practitioners of information, network, and computer-based physical security.
Denial of Service (DoS)	An attempt to make a network resource unavailable to its intended users.
Dynamic Host configuration Protocol (DHCP)	The protocol used to assign IP addresses to all nodes on the network.
Extensible Authentication Protocol (EAP)	A universal authentication framework frequently used in wireless networks and point-to-point connections.
Federal Bureau of Investigation (FBI)	A federal criminal investigation, intelligence agency, and the primary investigative arm of the United States Department of Justice.
Integrity Check Value (ICV)	A checksum or message footprint that allows an information technology system to detect changes or errors in data.

Institute of Electrical and Electronics Engineers (IEEE)	A worldwide professional association for electrical and electronics engineers that sets standards for telecommunications and computing applications.
IP Security (IPSec)	A suite of protocols for securing Internet Protocol communications by authenticating and/or encrypting each IP packet in a data stream.
Layer 2 Tunneling Protocol (L2TP)	A tunneling protocol used to support virtual private networks (VPNs).
MultiProtocol Label Switching (MPLS)	A data-carrying mechanism that emulates some properties of a circuit-switched network over a packet-switched network.
National Institute of Standards and Technology (NIST)	A non-regulatory agency of the United States Department of Commerce's Technology Administration.
Point-to-Point Tunneling Protocol (PPTP)	A method of implementing virtual private networks (VPNs).
Remote Address Dial-In User Service (RADIUS)	An AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility.
Rivest Cipher 4 (RC4)	The most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks).
SysAdmin Audit Network Security Institute (SANS)	An institute that provides computer security training, professional certification, and a research archive.
Sockets (SOCKS)	An Internet protocol that allows client-server applications to transparently use the services of a network firewall.
Secure Shell (SSH)	A set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer.

Secure Sockets Layer (SSL)	A cryptographic protocol used to validate the identity of a Web site and to create an encrypted connection.
Temporal Key Integrity Protocol (TKIP)	A security protocol used in Wi-Fi Protected Access (WPA).
Transport Secure Layer (TSL)	A security protocol based on the Secure Sockets Layer (SSL), which uses digital certificates to authenticate users as well as authenticate the network.
Virtual Private Network (VPN)	A private communications network used to communicate confidentiality over a public network.
War Driving	An act of an unauthorized person hacking a wireless data network in an attempt to log and collection information from the wireless access points.
Wired Equivalent Privacy (WEP)	A security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected to a wired LAN.
WiPhishing	An act of falsely obtaining user information by eavesdropping or sniffing wireless network traffic.
Wireless Local Area Network (WLAN)	A local area network that transmits over the air typically in the 2.4GHz or 5GHz unlicensed frequency band.
Wi-Fi Protected Access (WPA)	A security standard for wireless networks that provides strong data protection and network access control, created in response to several serious weaknesses of WEP.



## **Appendix B – Acronyms and Abbreviations**

AES	Advanced Encryption Standard
AP	Access Point
ATM	Asynchronous Transfer Mode
CCM	Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC)
CCMP	Counter Mode with CBC-MAC Protocol (CRT/CBC-MAC Protocol)
CSI	Computer Security Institute
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FBI	Federal Bureau of Investigation
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IPSec	IP Security
IS	Information Services
IT	Information Technology
L2TP	Layer 2 Tunneling Protocol
MPLS	MultiProtocol Label Switching
NIST	National Institute of Standards and Technology
PDA	Personal Digital Assistant
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Address Dial-In User Service
RC4	Rivest Cipher 4 (A Stream Cipher)
SANS	SysAdmin Audit Network Security Institute
SOCKS	Sockets
SSH	Secure Shell
SSL	Secure Sockets Layer
SWOT	Strengths, Weaknesses, Opportunities and Threats
TKIP	Temporal Key Integrity Protocol
TSL	Transport Secure Layer

UN/PW	User Name and Password
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

## Appendix C – Information Privacy and Security Awareness Survey



As you know, identity theft is the nation's faster growing crime where someone steals your personal information and uses it for financial gain. With today's convenience of wireless access to your online banking, e-commerce sites and other financial related transactions, we are more vulnerable than ever to tech-savvy thieves.

Please indicate your profession

- ☐ Student                      ☐ Staff                      ☐ Faculty  
☐ Others .....

Please check ONE that applies to your answer.

1. How important do you think the security of the wireless data network or Wi-Fi network you are using on campus should be?

- ☐ Not important  
☐ Somewhat important  
☐ Very important  
☐ Extremely important



With weak wireless network security, malicious intruders can possibly...

- Intercept your confidential data that you are sending from your wireless device, such as laptop and PDA.
- Read and modify your e-mail message before sending it again.
- Access your computer and sabotage anything on it, including hardware.

2. How much are you concerned with those threats while using the wireless service on campus?

- ☐ Not concerned  
☐ Somewhat concerned  
☐ Very concerned  
☐ Extremely concerned

3. On a scale 1 to 5, where 1 is the lowest and 5 is the highest, how much do you know about protecting yourself and your computer or PDA from those threats?

- ☐ 1                      ☐ 2                      ☐ 3                      ☐ 4                      ☐ 5  
(Don't know)      (A little)              (Moderate)              (Good)              (Excellent)

4. Which of the following wireless security technologies would you prefer?
- ☐ Low security protection. Very easy to access (only user name and password required).
  - ☐ High security protection. Initial security setup required. Software and/or firmware upgrade may be required.
  - ☐ Very high security protection. Initial security setup required. Software and/or firmware upgrade may be required. Some wireless terminals, such as PDAs and laptops with old operating systems, are not supported in this type of wireless network.

---

If you have any comments or suggestions, please feel free to let us know



Thank you for participating in our survey



## Appendix D – Raw Data Obtained from the Survey

Day 1: March 5 2007

Survey No.	Result	Question-1	Question-2	Question-3	Question-4
1	4332	4	3	3	2
2	4322	4	3	2	2
3	4232	4	2	3	2
4	4432	4	4	3	2
5	4322	4	3	2	2
6	3232	3	2	3	2
7	2223	2	2	2	3
8	2342	2	3	4	2
9	4232	4	2	3	2
10	2332	2	3	3	2
11	4423	4	4	2	3
12	2241	2	2	4	1
13	3342	3	3	4	2
14	2251	2	2	5	1
15	4332	4	3	3	2
16	3222	3	2	2	2
17	4433	4	4	3	3
18	4232	4	2	3	2
19	3232	3	2	3	2
20	3332	3	3	3	2
21	4413	4	4	1	3
22	3331	3	3	3	1
23	4332	4	3	3	2
24	4323	4	3	2	3
25	2131	2	1	3	1
26	4332	4	3	3	2
27	3232	3	2	3	2
28	3232	3	2	3	2
29	4441	4	4	4	1
30	3222	3	2	2	2

Day 2: March 6 2007

31	3242	3	2	4	2
32	1121	1	1	2	1
33	2232	2	2	3	2
34	3323	3	3	2	3
35	3331	3	3	3	1
36	3231	3	2	3	1
37	4342	4	3	4	2
38	4342	4	3	4	2
39	3231	3	2	3	1
40	3242	3	2	4	2
41	3243	3	2	4	3
42	3241	3	2	4	1
43	4332	4	3	3	2
44	4322	4	3	2	2
45	4351	4	3	5	1
46	3222	3	2	2	2
47	2223	2	2	2	3
48	2332	2	3	3	2
49	2351	2	3	5	1
50	3322	3	3	2	2
51	3232	3	2	3	2
52	4323	4	3	2	3
53	4342	4	3	4	2
54	2131	2	1	3	1
55	3332	3	3	3	2
56	4342	4	3	4	2
57	4341	4	3	4	1
58	3232	3	2	3	2
59	2241	2	2	4	1
60	3231	3	2	3	1

Day 3: March 7 2007

61	3232	3	2	3	2
62	3241	3	2	4	1
63	3322	3	3	2	2
64	4252	4	2	5	2
65	2332	2	3	3	2
66	2223	2	2	2	3
67	3332	3	3	3	2
68	3231	3	2	3	1
69	1221	1	2	2	1
70	3342	3	3	4	2
71	4341	4	3	4	1
72	4343	4	3	4	3
73	4322	4	3	2	2
74	4423	4	4	2	3
75	2341	2	3	4	1
76	2342	2	3	4	2
77	2351	2	3	5	1
78	3243	3	2	4	3
79	3232	3	2	3	2
80	3222	3	2	2	2
81	2342	2	3	4	2
82	2223	2	2	2	3
83	4342	4	3	4	2
84	3241	3	2	4	1
85	2131	2	1	3	1
86	2141	2	1	4	1
87	4441	4	4	4	1
88	3231	3	2	3	1
89	3342	3	3	4	2
90	4413	4	4	1	3

Day 4: March 8 2007

91	4252	4	2	5	2
92	3442	3	4	4	2
93	4421	4	4	2	1
94	3422	3	4	2	2
95	3222	3	2	2	2
96	4243	4	2	4	3
97	3332	3	3	3	2
98	2151	2	1	5	1
99	4432	4	4	3	2
100	3211	3	2	1	1
101	4343	4	3	4	3
102	3243	3	2	4	3
103	3323	3	3	2	3
104	4413	4	4	1	3
105	3232	3	2	3	2
106	4241	4	2	4	1
107	2222	2	2	2	2
108	4241	4	2	4	1
109	4252	4	2	5	2
110	3332	3	3	3	2
111	3231	3	2	3	1
112	3331	3	3	3	1
113	3323	3	3	2	3
114	2141	2	1	4	1
115	4252	4	2	5	2
116	4243	4	2	4	3
117	4341	4	3	4	1
118	2151	2	1	5	1
119	4232	4	2	3	2
120	3332	3	3	3	2



#### Summary of the Survey Question 1

Choices	Description	Count	Percentage
1	Not important	2	1.67%
2	Somewhat important	25	20.83%
3	Very important	48	40.00%
4	Extremely important	45	37.50%
<b>TOTAL</b>		<b>120</b>	<b>100.00%</b>

#### Summary of the Survey Question 2

Choices	Description	Count	Percentage
1	Not concerned	8	6.67%
2	Somewhat concerned	51	42.50%
3	Very concerned	48	40.00%
4	Extremely concerned	13	10.83%
<b>TOTAL</b>		<b>120</b>	<b>100.00%</b>

#### Summary of the Survey Question 3

Choices	Description	Count	Percentage
1	Don't know	4	3.33%
2	Little	27	22.50%
3	Moderate	43	35.83%
4	Good	36	30.00%
5	Excellent	10	8.33%
<b>TOTAL</b>		<b>120</b>	<b>100.00%</b>

#### Summary of the Survey Question 4

Choices	Description	Count	Percentage
1	Network Type A	37	30.83%
2	Network Type B	61	50.83%
3	Network Type C	22	18.33%
<b>TOTAL</b>		<b>120</b>	<b>100.00%</b>

## Appendix E – Statistical Calculations

### *Results from Survey Question 4*

Choices	Description	Count	Percentage
1	Network A	37	30.83%
2	Network B	61	50.83%
3	Network C	22	18.33%
<b>TOTAL</b>		<b>120</b>	<b>100.00%</b>

First, a confidence level has to be determined by setting a probability of error  $\alpha$  (Error Type I) of the survey. The author set  $\alpha = 5\%$ , assuming that 5% of the surveys will be meaningless.

$$\text{Confidence Level} = 100\% (1 - 0.05) = 95\%$$

According to the results of the survey question 4, 50.83% of the respondents or 61 wireless users prefer the wireless data network whose general characteristics are similar to the WPA-based wireless network.

$$\begin{aligned} \text{The sample proportion is } \pi &= 61/120 = 0.5083 \\ \text{Standard error of } \pi &= \sqrt{\pi(1 - \pi) / n} \quad ; n = \text{sample size} \\ &= \sqrt{0.5083 (1 - 0.5083) / 120} \\ &= 0.04563 \end{aligned}$$

At 95% confidence level

From the z-distribution table, the z value that cuts off a right-tail area of 0.025 is 1.96.

$$z_{\alpha/2} = z_{0.05/2} = 1.96$$

$$\begin{aligned} \text{So, margin of error} &= \pm \pi \cdot z_{\alpha/2} = \pm 1.96 \times 0.04563 \\ &= \pm 0.0894 \text{ or } \pm 8.94\% \end{aligned}$$

Statistically speaking, the maximum random sampling error occurs when the sample portion is 50%.

$$\begin{aligned} \text{The sample proportion is } \pi &= 60/120 = 0.50 \\ \text{Standard error of } \pi &= \sqrt{\pi(1 - \pi) / n} \quad ; n = \text{sample size} \\ &= \sqrt{0.50 (1 - 0.50) / 120} \\ &= 0.04564 \end{aligned}$$

At 95% confidence level

$$\begin{aligned} \text{So, margin of error} &= \pm \pi \cdot z_{\alpha/2} = \pm 1.96 \times 0.04564 \\ &= \pm 0.0895 \text{ or } \pm 8.95\% \end{aligned}$$

According to the statistical calculations above,

$$\begin{aligned} \text{The confidence level} &= 95\% \\ \text{The margin of error} &= \pm 8.95\% \end{aligned}$$